

全国计算机技术与软件专业技术资格（水平）考试指定用书

信息安全工程师考试大纲

2020年审定通过

全国计算机专业技术资格考试办公室　编

清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试指定用书

信息安全工程师考试大纲

全国计算机专业技术资格考试办公室　编

请编辑发排版时填写			
产品编号	打印时填入	组稿编辑	打印时填入
丛书名称	编辑填写		
正文印刷	□单色 □双色 □四色	文中插页	□黑白 □彩色 □无
成品尺寸	□203*260 □185*260 □186*240 □170*230 □145*210		
版　　式	□套书 □参照样书＿＿＿＿＿＿ □单本设计要求:		
是否要求排版软件	□无 □InDesign □Word □方正 □Latex		
附封面小样（必须是有复终审签字的小样）	□有 □否	封面工艺	□起亮 □亚光 □起鼓 □专色
刮刮卡	□有 □无	文稿编辑	编辑填写
请校对和印前流程时填写勾选		出作者样时间	
排版返回时间		出CTP时间	
核印张、附发稿封面小样填印单	□校对 □印前	附封面小样、扉页进入质检	□校对 □印前
排版要求：			

清华大学出版社

北　京

内 容 简 介

本书是全国计算机专业技术资格考试办公室组织编写的信息安全工程师考试大纲，本书除大纲内容外，还包括了人力资源和社会保障部、工业和信息化部的有关文件以及考试简介。

信息安全工程师考试大纲是针对本考试的信息系统中级资格制定的。通过本考试的考生，可被用人单位择优聘任为工程师。

图书在版编目(CIP)数据

信息安全工程师考试大纲 / 全国计算机专业技术资格考试办公室编. —北京：清华大学出版社，2020.8

全国计算机技术与软件专业技术资格（水平）考试指定用书

ISBN 978-7-302-50884-7

Ⅰ. ①信…　Ⅱ. ①全…　Ⅲ. ①信息安全—安全技术—资格考试—考试大纲　Ⅳ. ①TP309-41

中国版本图书馆 CIP 数据核字（2018）第 189850 号

责任编辑：杨如林
封面设计：常雪影
责任校对：胡伟民
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市龙大印装有限公司
经　　销：全国新华书店
开　　本：130mm×185mm　　**印　张：**2.125　　**字　数：**50 千字
版　　次：2020 年 9 月第 1 版　　**印　次：**2020 年 9 月第 1 次印刷
定　　价：15.00 元

产品编号：079253-01

前　　言

全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）是由人力资源和社会保障部、工业和信息化部领导的专业技术资格考试，属于国家职业资格考试。原人事部、信息产业部联合颁发的国人部发〔2003〕39号文件规定了这种考试的政策。计算机软件考试包括了计算机软件、计算机网络、计算机应用、信息系统、信息服务等领域初级资格（技术员/助理工程师）、中级资格（工程师）、高级资格（高级工程师）的27种职业岗位。根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，系统分析师、软件设计师、网络工程师、数据库系统工程师、程序员考试标准已经实现了中国与日本互认；程序员和软件设计师考试标准已经实现了中国和韩国互认。

各种资格的考试大纲（考试标准）体现了相应职业岗位对知识与能力的要求。这些要求是由全国计算机专业技术资格考试办公室组织的全国相关企业、研究所、高校等许多专家，经调研很多相关企业的相应职业岗位，参考先进国家的有关考试标准，逐步提炼，反复讨论形成的。一般的做法是先确定相应职业岗位的工作流程，对每个工作阶段又划分多个关键性活动，对每项活动再列出所需的知识以及所需的能力要求，最后，汇总这些知识要求与能力要求，形成考试大纲。初级与中级资格考试一般包括基础知识与应用技术两大科目；高级资格考试一般包括综合知识、案例分析与论文三

大科目。

正由于考试大纲来源于职业岗位的要求，是考试命题的依据，才使这种考试成为了衡量考生是否具有职业岗位要求的一个检验标准，受到社会上各用人单位的广泛欢迎。20 多年的考试历史也证明，这种考试已经成为我国著名的 IT 考试品牌，并使大批合格人员得到了升职聘用，对国家信息化发挥了重要的作用。这就是广大在职人员以及希望从事相关专业工作的学生积极报考的原因。

关于计算机软件考试的其他信息见网站 www.ruankao.org.cn 中的资格考试栏目。

编　者

2020 年 8 月

人事部
信息产业部 文件

国人部发〔2003〕39号

关于印发《计算机技术与软件专业技术资格（水平）考试暂行规定》和《计算机技术与软件专业技术资格（水平）考试实施办法》的通知

各省、自治区、直辖市人事厅（局）、信息产业厅（局），国务院各部委、各直属机构人事部门，中央管理的企业：

为适应国家信息化建设的需要，规范计算机技术与软件专业人才评价工作，促进计算机技术与软件专业人才队伍建设，人事部、信息产业部在总结计算机软件专业资格和水平考试实施情况的基础上，重新修订了计算机软件专业资格和水平考试有关规定。现将《计算机技术与软件专业技术资格（水平）考试暂行规定》和《计算机技术与软件专业技术资格（水平）考试实施办法》

印发给你们，请遵照执行。

自 2004 年 1 月 1 日起，人事部、原国务院电子信息系统推广应用办公室发布的《关于印发〈中国计算机软件专业技术资格和水平考试暂行规定〉的通知》（人职发〔1991〕6 号）和人事部《关于非在职人员计算机软件专业技术资格证书发放问题的通知》（人职发〔1994〕9 号）即行废止。

中华人民共和国　　中华人民共和国
人　事　部　　信息产业部

二〇〇三年十月十八日

计算机技术与软件专业技术资格（水平）考试暂行规定

第一条　为适应国家信息化建设的需要，加强计算机技术与软件专业人才队伍建设，促进我国计算机应用技术和软件产业的发展，根据国务院《振兴软件产业行动纲要》以及国家职业资格证书制度的有关规定，制定本规定。

第二条　本规定适用于社会各界从事计算机应用技术、软件、网络、信息系统和信息服务等专业技术工作的人员。

第三条　计算机技术与软件专业技术资格（水平）考试（以下简称计算机专业技术资格（水平）考试），纳入全国专业技术人员职业资格证书制度统一规划。

第四条　计算机专业技术资格（水平）考试工作由人事部、信息产业部共同负责，实行全国统一大纲、统一试题、统一标准、统一证书的考试办法。

第五条　人事部、信息产业部根据国家信息化建设和信息产业市场需求，设置并确定计算机专业技术资格（水平）考试专业类别和资格名称。

计算机专业技术资格（水平）考试级别设置：初级资格、中级资格和高级资格3个层次。

第六条 信息产业部负责组织专家拟订考试科目、考试大纲和命题，研究建立考试试题库，组织实施考试工作和统筹规划培训等有关工作。

第七条 人事部负责组织专家审定考试科目、考试大纲和试题，会同信息产业部对考试进行指导、监督、检查，确定合格标准。

第八条 凡遵守中华人民共和国宪法和各项法律，恪守职业道德，具有一定计算机技术应用能力的人员，均可根据本人情况，报名参加相应专业类别、级别的考试。

第九条 计算机专业技术资格（水平）考试合格者，由各省、自治区、直辖市人事部门颁发人事部统一印制，人事部、信息产业部共同用印的《中华人民共和国计算机专业技术资格（水平）证书》。该证书在全国范围有效。

第十条 通过考试并获得相应级别计算机专业技术资格（水平）证书的人员，表明其已具备从事相应专业岗位工作的水平和能力，用人单位可根据《工程技术人员职务试行条例》有关规定和工作需要，从获得计算机专业技术资格（水平）证书的人员中择优聘任相应专业技术职务。

取得初级资格可聘任技术员或助理工程师职务；取

得中级资格可聘任工程师职务；取得高级资格可聘任高级工程师职务。

第十一条 计算机专业技术资格（水平）实施全国统一考试后，不再进行计算机技术与软件相应专业和级别的专业技术职务任职资格评审工作。

第十二条 计算机专业技术资格（水平）证书实行定期登记制度，每 3 年登记一次。有效期满前，持证者应按有关规定到信息产业部指定的机构办理登记手续。

第十三条 申请登记的人员应具备下列条件：

（一）取得计算机专业技术资格（水平）证书；

（二）职业行为良好，无犯罪记录；

（三）身体健康，能坚持本专业岗位工作；

（四）所在单位考核合格。

再次登记的人员，还应提供接受继续教育或参加业务技术培训的证明。

第十四条 对考试作弊或利用其他手段骗取《中华人民共和国计算机专业技术资格（水平）证书》的人员，一经发现，即行取消其资格，并由发证机关收回证书。

第十五条 获准在中华人民共和国境内就业的外籍人员及港、澳、台地区的专业技术人员，可按照国家有关政策规定和程序，申请参加考试和办理登记。

第十六条 在本规定施行日前，按照《中国计算机软件专业技术资格和水平考试暂行规定》（人职发〔1991〕6 号）参加考试并获得人事部印制、人事部和

信息产业部共同用印的《中华人民共和国专业技术资格证书》（计算机软件初级程序员、程序员、高级程序员资格）和原中国计算机软件专业技术资格（水平）考试委员会统一印制的《计算机软件专业水平证书》的人员，其资格证书和水平证书继续有效。

第十七条 本规定自 2004 年 1 月 1 日起施行。

计算机技术与软件专业技术资格（水平）考试实施办法

第一条 计算机技术与软件专业技术资格（水平）考试（以下简称计算机专业技术资格（水平）考试）在人事部、信息产业部的领导下进行，两部门共同成立计算机专业技术资格（水平）考试办公室（设在信息产业部），负责计算机专业技术资格（水平）考试实施和日常管理工作。

第二条 信息产业部组织成立计算机专业技术资格（水平）考试专家委员会，负责考试大纲的编写、命题、建立考试试题库。

具体考务工作由信息产业部电子教育中心（原中国计算机软件考试中心）负责。各地考试工作由当地人事行政部门和信息产业行政部门共同组织实施，具体职责分工由各地协商确定。

第三条 计算机专业技术资格（水平）考试原则上每年组织两次，在每年第二季度和第四季度举行。

第四条 根据《计算机技术与软件专业技术资格（水平）考试暂行规定》（以下简称《暂行规定》）第五

条规定，计算机专业技术资格（水平）考试划分为计算机软件、计算机网络、计算机应用技术、信息系统和信息服务5个专业类别，并在各专业类别中分设了高、中、初级专业资格考试，详见《计算机技术与软件专业技术资格（水平）考试专业类别、资格名称和级别层次对应表》（附后）。人事部、信息产业部将根据发展需要适时调整专业类别和资格名称。

考生可根据本人情况选择相应专业类别、级别的专业资格（水平）参加考试。

第五条　高级资格设：综合知识、案例分析和论文3个科目；中级、初级资格均设：基础知识和应用技术2个科目。

第六条　各级别考试均分2个半天进行。

高级资格综合知识科目考试时间为2.5小时，案例分析科目考试时间为1.5小时、论文科目考试时间为2小时。

初级和中级资格各科目考试时间均为2.5小时。

第七条　计算机专业技术资格（水平）考试根据各级别、各专业特点，采取纸笔、上机或网络等方式进行。

第八条　符合《暂行规定》第八条规定的人员，由本人提出申请，按规定携带身份证明到当地考试管理机构报名，领取准考证。凭准考证、身份证明在指定的时间、地点参加考试。

第九条　考点原则上设在地市级以上城市的大、中

专院校或高考定点学校。

中央和国务院各部门所属单位的人员参加考试，实行属地化管理原则。

第十条 坚持考试与培训分开的原则，凡参与考试工作的人员，不得参加考试及与考试有关的培训。

应考人员参加培训坚持自愿的原则。

第十一条 计算机专业技术资格（水平）考试大纲由信息产业部编写和发行。任何单位和个人不得盗用信息产业部名义编写、出版各种考试用书和复习资料。

第十二条 为保证培训工作健康有序进行，由信息产业部统筹规划培训工作。承担计算机专业技术资格（水平）考试培训的机构，应具备师资、场地、设备等条件。

第十三条 计算机专业技术资格（水平）考试、登记、培训及有关项目的收费标准，须经当地价格行政部门核准，并向社会公布，接受群众监督。

第十四条 考务管理工作要严格执行考务工作的有关规章和制度，切实做好试卷的命制、印刷、发送和保管过程中的保密工作，遵守保密制度，严防泄密。

第十五条 加强对考试工作的组织管理，认真执行考试回避制度，严肃考试工作纪律和考场纪律。对弄虚作假等违反考试有关规定者，要依法处理，并追究当事人和有关领导的责任。

附表（已按国人厅发〔2007〕139号文件更新）

计算机技术与软件专业技术资格（水平）考试专业类别、资格名称和级别对应表

资格名称 \ 专业类别 / 级别层次	计算机软件	计算机网络	计算机应用技术	信息系统	信息服务
高级资格	• 信息系统项目管理师 • 系统分析师 • 系统架构设计师 • 网络规划设计师 • 系统规划与管理师				
中级资格	• 软件评测师 • 软件设计师 • 软件过程能力评估师	• 网络工程师	• 多媒体应用设计师 • 嵌入式系统设计师 • 计算机辅助设计师 • 电子商务设计师	• 系统集成项目管理工程师 • 信息系统监理师 • 信息安全工程师 • 数据库系统工程师 • 信息系统管理工程师	• 计算机硬件工程师 • 信息技术支持工程师
初级资格	• 程序员	• 网络管理员	• 多媒体应用制作技术员 • 电子商务技术员	• 信息系统运行管理员	• 网页制作员 • 信息处理技术员

主题词：专业技术人员 考试 规定 办法 通知

抄送：党中央各部门、全国人大常委会办公厅、全国政协办公厅、国务院办公厅、高法院、高检院、解放军各总部。

人事部办公厅 2003 年 10 月 27 日印发

全国计算机软件考试办公室文件

软考办〔2005〕1号

关于中日信息技术考试标准互认有关事宜的通知

各地计算机软件考试实施管理机构:

为进一步加强我国信息技术人才培养和选拔的标准化，促进国际间信息技术人才的流动，推动中日两国信息技术的交流与合作，信息产业部电子教育中心与日本信息处理技术人员考试中心，分别受信息产业部、人事部和日本经济产业省委托，就中国计算机技术与软件专业技术资格（水平）考试与日本信息处理技术人员考试（以下简称中日信息技术考试）的考试标准，于2005年3月3日再次签署了《关于中日信息技术考试标准互认的协议》，在2002年签署的互认协议的基础上增加了网络工程师和数据库系统工程师的互认。现就中日信息技术考试标准互认中的有关事宜内容通知如下:

一、中日信息技术考试标准互认的级别如下:

中国的考试级别 （考试大纲）	日本的考试级别 （技能标准）
系统分析师	系统分析师 项目经理 应用系统开发师
软件设计师	软件开发师
网络工程师	网络系统工程师
数据库系统工程师	数据库系统工程师
程序员	基本信息技术师

二、采取灵活多样的方式，加强对中日信息技术考试标准互认的宣传，不断扩大考试规模，培养和选拔更多的信息技术人才，以适应日益增长的社会需求。

三、根据国内外信息技术的迅速发展，继续加强考试标准的研究与更新，提高考试质量，进一步树立考试的品牌。

四、鼓励相关企业以及研究、教育机构，充分利用中日信息技术考试标准互认的新形势，拓宽信息技术领域国际交流合作的渠道，开展多种形式的国际交流与合作活动，发展对日软件出口。

五、以中日互认的考试标准为参考，引导信息技术领域的职业教育、继续教育改革，使其适应新形势下的职业岗位实际工作要求。

二〇〇五年三月八日

全国计算机软件考试办公室文件

软考办〔2006〕2号

关于中韩信息技术考试标准互认有关事宜的通知

各地计算机软件考试实施管理机构：

为加强我国信息技术人才培养和选拔的标准化，促进国际间信息技术人才的流动，推动中韩两国间信息技术的交流与合作，信息产业部电子教育中心与韩国人力资源开发服务中心，分别受信息产业部和韩国信息与通信部的委托，对中国计算机技术与软件专业技术资格（水平）考试与韩国信息处理技术人员考试（以下简称中韩信息技术考试）的考试标准进行了全面、认真、科学的分析比较，于2006年1月19日签署了《关于中韩信息技术考试标准互认的协议》，实现了程序员、软件设计师考试标准的互认，现将中韩信息技术考试标准互认的有关事宜通知如下：

一、中韩信息技术考试标准互认的级别如下：

中国的考试级别 （考试大纲）	韩国的考试级别 （技能标准）
软件设计师	信息处理工程师
程序员	信息处理产业工程师

二、各地应以中韩互认的考试标准为参考，积极引导信息技术领域的职业教育发展，使其适应新形势下的职业岗位的要求。

三、鼓励相关企业以及研究、教育机构，充分利用中韩信息技术考试标准互认的新形势，拓宽信息技术领域国际交流合作的渠道，开展多种形式的国际交流与合作活动，发展对韩软件出口。

四、根据国内外信息技术的迅速发展，加强考试标准的研究与更新，提高考试质量，进一步树立考试的品牌。

五、各地应采取灵活多样的方式，加强对中韩信息技术考试标准互认的宣传，不断扩大考试规模，培养和选拔更多的信息技术人才，以适应日益增长的社会需求。

二〇〇六年二月五日

全国计算机技术与软件专业技术资格（水平）考试简介

全国计算机技术与软件专业技术资格（水平）考试（简称计算机软件考试）是在人力资源和社会保障部、工业和信息化部领导下的国家考试，其目的是，科学、公正地对全国计算机技术与软件专业技术人员进行职业资格、专业技术资格认定和专业技术水平测试。

计算机软件考试在全国范围内已经实施了二十多年，年考试规模已超过三十万人。该考试由于其权威性和严肃性，得到了社会及用人单位的广泛认同，并为推动我国信息产业特别是软件产业的发展和提高各类 IT 人才的素质做出了积极的贡献。

根据人事部、信息产业部文件（国人部发〔2003〕39 号），计算机软件考试纳入全国专业技术人员职业资格证书制度的统一规划。通过考试获得证书的人员，表明其已具备从事相应专业岗位工作的水平和能力，用人单位可根据工作需要从获得证书的人员中择优聘任相应专业技术职务（技术员、助理工程师、工程师、高级工程师）。计算机技术与软件专业实施全国统一考试后，不再进行相应专业技术职务任职资格的评审工作。因

此，这种考试既是职业资格考试，又是专业技术资格考试。报考任何级别不需要学历、资历条件，考生可根据自己熟悉的专业情况和水平选择适当的级别报考。程序员、软件设计师、系统分析师、网络工程师、数据库系统工程师的考试标准已与日本相应级别实现互认，程序员和软件设计师的考试标准还实现了中韩互认，以后还将扩大考试互认的级别以及互认的国家。

本考试分 5 个专业类别：计算机软件、计算机网络、计算机应用技术、信息系统和信息服务。每个专业又分 3 个层次：高级资格（高级工程师）、中级资格（工程师）、初级资格（助理工程师、技术员）。对每个专业、每个层次，设置了若干个资格（或级别）。

考试合格者将颁发由人力资源和社会保障部、工业和信息化部用印的计算机技术与软件专业技术资格（水平）证书。

本考试每年分两次举行。每年上半年和下半年考试的级别不尽相同。考试大纲、指定教材、辅导用书由全国计算机专业技术资格考试办公室组编陆续出版。

关于考试的具体安排、考试用书、各地报考咨询联系方式等都在网站 www.ruankao.org.cn 公布。在该网站上还可以查询证书的有效性。

信息安全工程师考试大纲

一、考 试 说 明

1．考试目标

通过本考试的合格人员能够掌握网络信息安全的基础知识和技术原理；根据国家网络信息安全相关法律法规及业务安全保障要求，能够规划、设计信息系统安全方案，能够配置和维护常见的网络安全设备及系统；能够对信息系统的网络安全风险进行监测和分析，并给出网络安全风险问题的整改建议；能够协助相关部门对单位的信息系统进行网络安全审计和网络安全事件调查；能够对网络信息安全事件开展应急处置工作；具有工程师的实际工作能力和业务水平。

2．考试要求

（1）熟悉网络信息安全的机密性、可用性、完整性等基本知识，了解个人信息隐私保护的概念；

（2）熟悉网络信息系统的身份认证、访问控制、日志审计、安全监控工作机制和技术原理；

（3）掌握密码体制、密码算法、密码威胁、密码应用等基本知识与技术，熟悉数据加密、SSL、VPN、数字签名、PKI 等密码应用工作原理；

（4）掌握网络安全威胁工作原理，理解端口扫描、口令破解、缓冲区溢出、计算机病毒、网络蠕虫、特洛伊木马、

僵尸网络、网站假冒、拒绝服务、网络嗅探、SQL 注入等网络安全威胁相关知识；

（5）掌握防火墙、漏洞扫描、VPN、物理隔离、入侵检测、入侵防御、系统安全增强、安全审计、可信计算、隐私保护、数字水印、安全风险评估、安全应急响应等网络安全技术原理及应用；

（6）熟悉网络信息安全风险评估工作机制，了解物理环境、计算机、操作系统、数据库、应用系统、网站、智能手机、互联网、移动应用、云计算、物联网、工业控制、大数据、智能设备、机器学习等领域的安全风险，能够提出网络信息安全技术和管理解决方案，能够理解和分析评估网络安全厂商的产品技术方案；

（7）能够阅读网络信息安全等级保护标准和相关规范，能够理解相关技术标准要求；

（8）能够阅读和理解网络信息安全相关的法律法规、管理规定；

（9）熟练阅读和正确理解网络信息安全相关领域的科技英文资料，了解物联网、云计算、人工智能、大数据等新兴技术的网络安全风险。

3．考试科目设置

（1）网络信息安全基础知识和技术，考试时间为 150 分钟，笔试，选择题；

（2）网络信息安全工程与综合应用实践，考试时间为 150 分钟，笔试，问答题。

二、考 试 范 围

考试科目 1：网络信息安全基础知识和技术

1. 网络信息安全概述

1.1　网络信息安全基本属性

- 机密性
- 完整性
- 可用性
- 抗抵赖性
- 可控性
- 其他（真实性、时效性、合规性、隐私性、公平性等）

1.2　网络信息安全现状与问题

- 网络信息安全现状
- 网络信息安全问题

1.3　网络信息安全目标与功能

- 网络信息安全目标
- 网络信息安全功能

1.4　网络信息安全基本技术需求

- 物理环境安全
- 网络信息安全认证
- 网络信息访问控制
- 网络信息安全保密与内容安全
- 网络信息安全监测与预警
- 网络信息安全漏洞扫描与安全评估

- 恶意代码监测与防护
- 网络信息安全应急响应

1.5 网络信息安全管理内容与方法

- 网络信息安全管理目标
- 网络信息安全管理对象
- 网络信息安全管理要素
- 网络信息安全管理依据
- 网络信息安全管理方法
- 网络信息安全管理流程
- 网络信息安全管理工具

1.6 网络信息安全法律与政策文件

- 国家网络空间安全战略
- 网络信息安全基本法律
- 网络安全等级保护
- 国家密码管理制度
- 网络产品和服务审查
- 互联网域名安全管理
- 工业控制信息安全制度
- 个人信息和重要数据保护制度
- 网络安全标准规范与测评
- 网络安全事件与应急响应制度

1.7 网络信息安全科技信息获取

- 网络信息安全会议
- 网络信息安全期刊
- 网络信息安全网站
- 网络信息安全术语

2. 网络攻击原理与常用方法

2.1 网络攻击概述

- 网络攻击概念
- 网络攻击模型
- 网络攻击发展演变

2.2 网络攻击一般过程

- 隐藏攻击源
- 收集攻击目标信息
- 挖掘漏洞信息
- 获取目标访问权限
- 隐蔽攻击行为
- 实施攻击
- 开辟后门
- 清除攻击痕迹

2.3 网络攻击常见技术方法

- 端口扫描
- 口令破解
- 缓冲区溢出
- 恶意代码（计算机病毒、网络蠕虫、特洛伊木马等）
- 网站假冒
- 网络钓鱼
- 拒绝服务
- 网络嗅探
- 网络窃听
- SQL 注入攻击
- 社交工程方法

- 会话劫持
- 漏洞扫描
- 代理技术
- 数据加密技术

2.4 黑客常用软件

- 扫描类软件
- 远程监控类软件
- 密码破解类软件
- 网络嗅探类软件

2.5 网络攻击案例

- 网络端口扫描
- DoS/DDoS
- 恶意代码
- 操作系统攻击
- 数据库攻击
- 网站及 Web 应用攻击

3. 密码学基本理论

3.1 密码学概况

- 密码学发展简况
- 密码学基本概念
- 密码安全性分析

3.2 密码体制分类

- 私钥密码体制
- 公钥密码体制
- 混合密码体制

3.3 常用密码算法

- DES 密码算法

- IDEA 密码算法
- AES 密码算法
- RSA 密码算法
- 国产密码算法

3.4 Hash 函数与数字签名

- Hash 函数的工作原理
- 常见的 Hash 算法
- 数字签名的概念及作用
- 数字签名的工作原理
- 数字签名的相关算法

3.5 密码管理与数字证书

- 密码管理
- 数字证书

3.6 安全协议

- SSL
- SSH
- Diffie–Hellman 密钥交换协议

3.7 密码学网络安全应用

- 密码技术主要应用场景类型
- 路由器安全应用
- 网站安全应用
- 电子邮件安全应用

4. 网络安全体系与网络安全模型

4.1 网络安全体系概述

- 网络安全体系概念
- 网络安全体系特征
- 网络安全体系用途

4.2 网络安全体系相关安全模型

- BLP 机密性模型
- BiBa 完整性模型
- 信息流模型
- 信息保障模型
- 能力成熟度模型
- 纵深防御模型
- 分层防护模型
- 等级保护模型
- 网络生存模型

4.3 网络安全体系建设原则与安全策略

- 网络安全原则
- 网络安全策略

4.4 网络安全体系框架组成和建设内容

- 网络安全体系组成框架
- 网络安全组织体系构建内容
- 网络安全管理体系构建内容
- 网络安全技术体系构建内容
- 网络安全基础设施及网络安全服务构建内容
- 网络信息科技与产业生态构建内容
- 网络安全教育与培训构建内容
- 网络安全标准与规范构建内容
- 网络安全运营与应急响应构建内容
- 网络安全投入与建设构建内容

4.5 网络安全体系建设参考案例

- 网络安全组织体系建设参考案例
- 网络安全管理体系建设参考案例

- 网络安全技术体系建设参考案例
- 网络安全等级保护体系
- ISO 27000 信息安全管理标准

5. 物理与环境安全技术

5.1 物理安全概念与要求

- 物理安全概念
- 物理安全要求

5.2 物理环境安全分析与防护

- 自然灾害防护（防水、防雷、防震等）
- 人为破坏及鼠虫害安全防护
- 电磁及供电安全防护（防电磁、防静电、安全供电等）

5.3 机房安全分析与防护

- 机房组成内容
- 机房安全等级
- 机房场地选择

5.4 网络通信线路安全分析与防护

- 网络通信线路安全分析
- 网络通信线路安全防护

5.5 设备实体安全分析与防护

- 设备实体安全分析
- 设备实体安全防护

5.6 存储介质安全分析与防护

- 存储介质安全分析
- 存储介质安全防护

6. 认证技术原理与应用

6.1 认证概述

- 认证概念
- 认证依据
- 认证原理

6.2 认证类型与认证过程

- 单向认证
- 双向认证
- 第三方认证

6.3 认证技术方法

- 口令认证技术
- 智能卡技术
- 基于生物特征认证技术
- Kerberos 认证技术
- 公钥基础设施（PKI）技术
- 单点登录

6.4 认证主要技术指标与产品

- 认证主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 认证产品（认证产品工作机制分析、认证产品标准理解、认证产品适用场景等）

6.5 认证技术应用

- 用户身份验证
- 信息来源证实
- 信息安全保护

7. 访问控制技术原理与应用

7.1 访问控制概述

- 访问控制概念
- 访问控制目标

7.2 访问控制模型

- 访问控制模型组成要素（主体、客体、参考监视器、访问控制数据库、审计库）
- 访问控制模型运行机制

7.3 访问控制类型

- 自主访问控制
- 强制访问控制
- 基于角色的访问控制

7.4 访问控制策略设计与实现

- 访问控制策略（访问控制策略定义、访问控制策略实现、访问控制策略类型、机密性访问策略、完整性访问策略等）
- 访问控制规则类型及实施方法（基于用户身份、基于角色、基于地址、基于时间、基于异常事件、基于服务数量等）

7.5 访问控制过程与安全管理

- 访问控制管理过程
- 最小特权管理
- 用户访问管理
- 口令管理

7.6 访问控制主要技术指标与产品

- 产品的访问控制机制分析
- 产品的主要功能指标分析
- 产品的主要性能指标分析

7.7 访问控制技术应用

- UNIX/Linux 操作系统访问控制应用
- Windows 操作系统访问控制应用

- Web 服务器访问控制应用
- 网络通信访问控制应用

8. 防火墙技术原理与应用

8.1 防火墙概述

- 防火墙概念
- 防火墙工作原理
- 防火墙安全隐患
- 防火墙发展

8.2 防火墙类型与实现技术

- 基于防火墙产品形态分类（软件防火墙、硬件防火墙）
- 基于防火墙应用领域分类（网络防火墙、Web 防火墙、工控防火墙）
- 防火墙实现技术（包过滤技术、应用服务代理技术、网络地址转换技术、Web 防火墙技术、数据库防火墙技术、工控防火墙技术、下一代防火墙技术等）

8.3 防火墙主要技术指标与产品

- 防火墙主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 防火墙产品工作机制分析、防火墙产品标准理解、防火墙产品适用场景等

8.4 防火墙技术应用

- 防火墙部署过程
- 恶意流量过滤应用
- 网站保护应用
- 网络安全区域隔离

9. VPN 技术原理与应用

9.1 VPN 概述

- VPN 概念
- VPN 工作原理
- VPN 安全服务功能

9.2 VPN 类型和实现技术

- VPN 类型（链路层 VPN、网络层 VPN、传输层 VPN 等）
- VPN 实现技术（密码算法、密钥管理、认证访问控制、IPSec 协议、SSL 协议等）

9.3 VPN 主要技术指标与产品

- VPN 主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- VPN 产品工作机制分析、VPN 产品标准理解、VPN 产品适用场景等

9.4 VPN 技术应用

- 远程安全访问
- 外部网络安全互联
- 构建内部安全专网

10. 入侵检测技术原理与应用

10.1 入侵检测概述

- 入侵检测概念
- 入侵检测模型
- 入侵检测作用

10.2 入侵检测技术

- 基于误用的入侵检测技术
- 基于异常的入侵检测技术

- 基于规范的检测方法
- 基于生物免疫的检测方法
- 基于攻击诱骗的检测方法
- 基于入侵报警的关联检测方法

10.3　入侵检测系统组成与分类

- 入侵检测系统组成
- 基于主机的入侵检测系统
- 基于网络的入侵检测系统
- 分布式入侵检测系统

10.4　入侵检测系统主要技术指标与产品

- 入侵检测主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 入侵检测产品工作机制分析、入侵检测产品标准理解、入侵检测产品适用场景等

10.5　入侵检测系统应用

- 入侵检测系统部署方法与步骤
- 主机入侵检测
- 网络系统内部入侵检测
- 网络系统外部入侵检测

11．网络物理隔离技术原理与应用

11.1　网络物理隔离概述

- 网络物理隔离概念
- 网络物理隔离工作原理

11.2　网络物理隔离系统与类型

- 网络物理隔离系统组成
- 双向网络物理隔离系统

- 单向网络物理隔离系统
- 终端物理隔离系统

11.3　网络物理隔离机制与实现技术

- 专用计算机
- 多 PC
- 外网代理服务
- 内外网线路切换器
- 单硬盘内外分区
- 双硬盘
- 网闸
- 协议隔离技术
- 单向传输部件
- 信息摆渡技术
- 物理断开技术

11.4　网络物理隔离主要技术指标与产品

- 网络物理隔离主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 网络物理隔离产品工作机制分析、网络物理隔离产品标准理解、网络物理隔离产品适用场景等

11.5　网络物理隔离应用

- 内网用户安全访问互联网
- 业务生产网与互联网隔离
- 内外网安全物理隔离
- 不同安全区域信息交换

12. 网络安全审计技术原理与应用

12.1 网络安全审计概述

- 网络安全审计概念
- 网络安全审计用途

12.2 网络安全审计系统组成与类型

- 网络安全审计系统组成
- 网络安全审计系统运行机制
- 网络安全审计系统类型（网络通信安全审计、操作系统安全审计、数据库安全审计、应用系统安全审计、运维安全审计等）

12.3 网络安全审计机制与实现技术

- 网络安全审计数据采集
  - 网络流量数据采集技术（交换机端口镜像、网络嗅探等）
  - 系统日志数据采集技术（Syslog、FTP、SNMP 等）
- 网络流量数据采集开源工具 Tcpdump 的使用
- 网络审计数据分析技术（字符串匹配、全文搜索、数据关联、统计报表、可视化分析等）
- 网络审计数据保护技术（系统用户分权管理、审计数据强制访问、审计数据加密、审计数据隐私保护、审计数据完整性保护、审计数据备份等）

12.4 网络安全审计主要技术指标与产品

- 网络安全审计主要技术指标（功能技术指

标理解、性能技术指标理解、安全技术指标理解等）

- 网络安全审计产品工作机制分析、网络安全审计产品标准理解、网络安全审计产品适用场景等

12.5 网络安全审计应用

- 网络合规使用
- 网络电子取证
- 网络安全运维保障

13. 网络安全漏洞防护技术原理与应用

13.1 网络安全漏洞概述

- 网络安全漏洞概念
- 网络安全漏洞危害（敏感信息泄露、普通用户权限提升、获取远程管理员权限、拒绝服务、服务器信息泄露、非授权访问、读取受限文件、身份假冒、口令恢复、欺骗等）
- 国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）等的漏洞标准规范

13.2 网络安全漏洞分类与管理

- 网络安全漏洞来源（非技术性安全漏洞和技术性安全漏洞）
  - ◆ 非技术性安全漏洞（网络安全责任主体不明、网络安全策略不完备、网络安全操作技能不足、网络安全监督缺失、网络安全特权控制不完备等）

- ◆ 技术性安全漏洞（设计错误、输入验证错误、缓冲区溢出、意外情况处置错误、访问验证错误、配置错误、竞争条件、环境错误等）
- 网络安全漏洞命名规范（CVE、CNNVD、CNVD 等）
- 网络安全漏洞分类分级（CNNVD 漏洞分级方法、通用漏洞计分系统、OWASP TOP 10 Web 应用漏洞等）
- 网络安全漏洞发布（漏洞发布方式、漏洞信息发布内容等）
- 网络安全漏洞获取（漏洞信息来源、漏洞信息内容等）
- 网络安全漏洞信息来源（国家信息安全漏洞库、国家信息安全漏洞共享平台、Bugtraq 漏洞库等）
- 网络安全漏洞管理过程（网络信息系统资产确认、网络安全漏洞信息采集、网络安全漏洞评估、网络安全漏洞消除和控制、网络安全漏洞变化跟踪等）

13.3　网络安全漏洞扫描技术与应用

- 主机漏洞扫描技术
- 网络漏洞扫描技术
- Web 漏洞扫描技术
- 数据库漏洞扫描技术
- 网络安全漏洞扫描应用

13.4　网络安全漏洞处置技术与应用

- 网络安全漏洞处置技术（网络安全漏洞发现技术、网络安全漏洞修补技术、网络安全漏洞利用防范技术等）
- 网络安全漏洞处置应用(服务器安全加固、网络设备安全加固等)

13.5 网络安全漏洞防护主要技术指标与产品

- 网络安全漏洞防护产品功能技术指标理解
- 网络安全漏洞防护产品性能技术指标理解
- 网络安全漏洞防护产品安全技术指标理解
- 网络安全漏洞防护产品工作机制分析
- 网络安全漏洞防护产品标准理解
- 网络安全漏洞防护产品适用场景

14. 恶意代码防范技术原理

14.1 恶意代码概述

- 恶意代码概念与分类
- 恶意代码攻击模型
- 恶意代码生存技术
- 恶意代码攻击技术
- 恶意代码分析技术
- 恶意代码防范策略

14.2 计算机病毒分析与防护

- 计算机病毒概念与特性
- 计算机病毒组成与运行机制
- 计算机病毒常见类型与技术(引导型病毒、宏病毒、多态病毒、隐蔽病毒等)
- 计算机病毒防范策略与技术（计算机病毒检测、计算机病毒防范、计算机病毒应急

响应等）
- 计算机病毒防护模式（基于单机计算机病毒防护、基于网络计算机病毒防护、基于网络分级病毒防护、基于邮件网关病毒防护、基于网关防护等）

14.3　特洛伊木马分析与防护
- 特洛伊木马概念与特性
- 特洛伊木马运行机制（特洛伊木马运行过程、特洛伊木马激活等）
- 特洛伊木马技术（特洛伊木马植入技术、特洛伊木马隐藏技术、特洛伊木马存活技术等）
- 特洛伊木马防范技术（基于查看开放端口检测特洛伊木马技术、基于重要系统文件检测特洛伊木马技术、基于系统注册表检测特洛伊木马技术、检测具有隐藏能力的特洛伊木马技术、基于网络检测特洛伊木马技术、基于网络阻断特洛伊木马技术、清除特洛伊木马技术等）

14.4　网络蠕虫分析与防护
- 网络蠕虫概念与特性
- 网络蠕虫组成部件与运行机制
- 网络蠕虫常用技术（网络蠕虫扫描技术、网络蠕虫漏洞利用技术等）
- 网络蠕虫防范技术（网络蠕虫监测与预警技术、网络蠕虫传播抑制技术、网络系统漏洞检测与系统加固技术、网络蠕虫免疫

技术、网络蠕虫阻断与隔离技术、网络蠕虫清除技术等）

14.5 僵尸网络分析与防护

- 僵尸网络概念与特性
- 僵尸网络运行机制与常用技术（通信内容加密、信息隐藏等）
- 僵尸网络防范技术（僵尸网络威胁监测、僵尸网络检测、僵尸网络主动遏制、僵尸程序查杀等）

14.6 其他恶意代码分析与防护

- 逻辑炸弹
- 陷门
- 细菌
- 间谍软件

14.7 恶意代码防护主要技术指标与产品

- 恶意代码防护主要技术指标（恶意代码检测能力、恶意代码检测准确性、恶意代码阻断能力等）
- 恶意代码防护产品（终端防护类产品、安全网关、恶意代码监测类产品、补丁管理、恶意代码应急响应等）

14.8 恶意代码防护技术应用

- 终端恶意代码防护
- 电子文档及电子邮件恶意代码防护

15. 网络安全主动防御技术原理与应用

15.1 入侵阻断技术与应用

- 入侵阻断技术原理

- 入侵阻断技术应用

15.2　软件白名单技术与应用

- 软件白名单技术原理
- 软件白名单技术应用

15.3　网络流量清洗技术与应用

- 网络流量清洗技术原理
- 网络流量清洗技术应用

15.4　可信计算技术与应用

- 可信计算技术原理
- 可信计算技术应用

15.5　数字水印技术与应用

- 数字水印技术原理
- 数字水印技术应用

15.6　网络攻击陷阱技术与应用

- 网络攻击陷阱技术原理
- 网络攻击陷阱技术应用

15.7　入侵容忍及系统生存技术与应用

- 入侵容忍及系统生存技术原理
- 入侵容忍及系统生存技术应用

15.8　隐私保护技术与应用

- 隐私保护技术原理
- 隐私保护技术应用

15.9　网络安全前沿技术发展动向

- 网络威胁情报服务
- 域名服务安全保障
- 同态加密技术

16. 网络安全风险评估技术原理与应用

16.1 网络安全风险评估概述

- 网络安全风险评估概念
- 网络安全风险评估要素
- 网络安全风险评估模式

16.2 网络安全风险评估过程

- 网络安全风险评估准备
- 网络资产识别
- 网络安全威胁识别
- 网络安全脆弱性识别
- 已有安全措施确认
- 网络安全风险计算与分析
- 网络安全风险应对措施

16.3 网络安全风险评估技术方法与工具

- 资产信息收集
- 网络拓扑发现
- 网络安全漏洞扫描
- 人工检查
- 网络安全渗透测试
- 问卷调查
- 网络安全访谈
- 审计数据分析
- 入侵监测

16.4 网络安全风险评估流程和工作内容

- 评估工程前期准备
- 评估方案设计与论证
- 评估方案实施

- 风险评估报告撰写
- 评估结果评审与认可

16.5　网络安全风险评估技术应用

- 网络安全风险评估应用场景
- OWASP 风险评估方法参考
- ICT 供应链安全威胁识别参考
- 工业控制系统平台脆弱性识别参考
- 网络安全风险处理措施参考
- 人工智能安全风险分析参考

17. 网络安全应急响应技术原理与应用

17.1　网络安全应急响应概述

- 网络安全应急响应概念
- 网络安全应急响应作用
- 网络安全应急响应相关规范

17.2　网络安全应急响应组织建立与工作机制

- 网络安全应急响应组织建立
- 网络安全应急响应组织工作机制
- 网络安全应急响应组织类型

17.3　网络安全应急响应预案内容与类型

- 网络安全事件类型与分级
- 网络安全应急响应预案基本内容
- 网络安全应急响应预案类型与参考模板

17.4　常见网络安全应急事件场景与处理流程

- 常见网络安全应急事件场景（恶意程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、自然灾害性事件等）

- 网络安全应急处理流程（安全事件报警、安全事件确认、启动应急预案、安全事件处理、撰写安全事件报告、应急工作总结等）
- 网络安全事件应急演练
  - 网络安全事件应急演练类型
  - 网络安全事件应急演练方法（如 CTF 夺旗比赛/红蓝对抗赛、网络攻防平台等）

17.5　网络安全应急响应技术与常见工具

- 访问控制（防火墙、VLAN、路由器的访问设置等）
- 网络安全评估（恶意代码检测、漏洞扫描、文件完整性检查、系统配置文件检查、网卡混杂模式检查、日志文件审查等）
- 网络安全监测
  - 网络流量监测及相关工具（TCPDump、WireShark、TCPView、netstat 等）
  - Windows 系统自身监测（系统进程管理工具——任务管理器、PsTools 等，网络连接状态检查及相关工具——netstat、net、fport 等）
  - UNIX/Linux 系统自身监测（系统进程管理工具 ps，网络连接状态检查及相关工具——netstat、lsof 等）
- 系统恢复（系统紧急启动、恶意代码清除、系统漏洞修补、文件删除恢复、系统备份容灾等）
- 入侵取证（证据信息来源、证据信息获取、

证据安全保护、证据分析以及相关工具，如 grep、find、OllyDbg、GDB、strings、tracert 等）

17.6 网络安全应急响应参考案例

- 公共互联网网络安全突发事件应急预案
- 网络安全应急响应服务
- 产品安全漏洞应急响应
- “永恒之蓝”攻击的紧急处置
- 页面篡改事件处置规程

18. 网络安全测评技术与标准

18.1 网络安全测评概况

- 网络安全测评概念
- 网络安全测评发展
- 网络安全测评作用

18.2 网络安全测评类型

- 基于测评目标分类（网络信息系统安全等级保护测评、网络信息系统安全验收测评、网络信息系统安全风险测评等）
- 基于测评内容分类（技术安全测评、管理安全测评等）
- 基于实施方式分类（安全功能检测、安全管理检测、代码安全审查、网络安全渗透、信息系统攻击测试等）
- 基于测评对象保密性分类（涉密信息系统测评、非涉密信息系统测评等）

18.3 网络安全测评流程与内容

- 网络安全等级保护测评流程与内容

- 技术安全测评的主要内容（安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心）
- 管理安全测评的主要内容（安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理）

- 网络安全渗透测试流程与内容
  - 网络安全渗透测试的过程（委托受理、准备、实施、综合评估、结题五个阶段）
  - 网络安全渗透测试内容（目标系统的信息收集、漏洞扫描及发现、漏洞分析及利用验证、漏洞风险处置与修补等）

18.4　网络安全测评技术与工具

- 漏洞扫描（网络安全漏洞扫描、主机安全漏洞扫描、数据库安全漏洞扫描、Web 应用安全漏洞扫描等）
- 安全渗透（安全渗透模型、安全渗透工具等）
- 代码安全审查（源代码、二进制代码等安全符合性检查）
- 协议分析（网络协议数据的获取和分析，协议分析常用工具 TCPDump、WireShark 等）
- 性能测试（性能监测工具、开源工具 Apache JMeter 等）

18.5　网络安全测评质量管理与标准

- 网络安全测评质量管理
  - 网络安全测评质量管理内容

- 网络安全测评质量管理参考标准
    - 网络安全测评相关机构认可管理
- 网络安全测评标准
    - 信息系统安全等级保护测评标准
    - 产品测评标准
    - 信息安全风险评估标准
    - 密码应用安全
    - 工业控制系统信息安全防护能力评估

19. 操作系统安全保护

19.1 操作系统安全概述

- 操作系统安全概念
- 操作系统安全需求
- 操作系统安全机制
- 操作系统安全技术

19.2 Windows 操作系统安全分析与防护

- Windows 操作系统安全分析（系统安全架构、系统安全机制、系统安全威胁分析等）
- Windows 操作系统安全防护（系统安全增强技术方法与流程、系统安全增强工具与产品、系统常见漏洞与解决方法等）

19.3 UNIX/Linux 操作系统安全分析与防护

- UNIX/Linux 操作系统安全分析（系统安全架构、系统安全机制、系统安全威胁分析等）
- UNIX/Linux 操作系统安全防护（系统安全增强方法和流程、系统安全增强工具与产品、系统常见漏洞与解决方法等）

19.4 国产操作系统安全分析与防护

- 国产操作系统概况
- 国产操作系统安全分析
- 国产操作系统安全增强措施

20．数据库系统安全

20.1　数据库安全概况

- 数据库安全概念
- 数据库安全威胁
- 数据库安全隐患
- 数据库安全需求

20.2　数据库安全机制与实现技术

- 数据库安全机制（标识与鉴别、访问控制、安全审计、备份与恢复、资源限制、安全加固、安全管理等）
- 数据库加密
- 数据库脱敏
- 数据库漏洞扫描
- 数据库防火墙

20.3　Oracle 数据库安全分析与防护

- Oracle 安全概况
- Oracle 安全分析
- Oracle 安全最佳实践
- Oracle 漏洞修补

20.4　MS SQL 数据库安全分析与防护

- MS SQL 安全概况
- MS SQL 安全分析
- MS SQL 安全最佳实践
- MS SQL 漏洞修补

20.5 MySQL 数据库安全分析与防护

- MySQL 安全概况
- MySQL 安全分析
- MySQL 安全最佳实践
- MySQL 漏洞修补

20.6 国产数据库安全分析与防护

- 国产数据库概况
- 国产数据库安全分析
- 国产数据库安全增强措施

21. 网络设备安全

21.1 网络设备安全概况

- 交换机安全威胁
- 路由器安全威胁

21.2 网络设备安全机制与实现技术

- 认证机制
- 访问控制
- 信息加密
- 安全通信
- 日志审计
- 安全增强
- 物理安全

21.3 网络设备安全增强技术方法

- 交换机安全增强技术方法（配置交换机访问口令和 ACL 以限制安全登录、利用镜像技术监测网络流量、MAC 地址控制技术、安全增强等）
- 路由器安全增强技术方法（及时升级操作

系统和打补丁、关闭不需要的网络服务、禁止 IP 直接广播和源路由、增强路由器 VTY 安全、阻断恶意数据包、路由器口令安全、传输加密、增强路由器 SNMP 的安全等）

21.4 网络设备常见漏洞与解决方法

- 网络设备常见漏洞（拒绝服务漏洞、跨站伪造请求、格式化字符串漏洞、XSS、旁路、代码执行、溢出、内存破坏等）
- 网络设备漏洞解决方法（及时获取网络设备漏洞信息、网络设备漏洞扫描、网络设备漏洞修补等）

22. 网络信息安全专业英语

- 具有工程师所要求的英语阅读水平
- 理解本领域的英语术语

考试科目 2：网络信息安全工程与综合应用实践

1. 网络安全风险评估与需求分析

1.1 网络安全风险评估实践

- 操作系统安全风险评估
- 数据库系统安全风险评估
- 网络设备及通信安全风险评估
- 应用系统安全风险评估
- 数据安全风险评估
- 物理安全风险评估

1.2 网络安全数据收集与分析

- syslog 日志数据采集

- 操作系统日志安全分析
- 数据库系统日志安全分析
- 网络设备日志安全分析
- 网络安全设备日志安全分析
- 网站日志安全分析
- 网络协议分析器安装和使用
- 网络协议数据安全分析

2. 网络安全常用方案设计

2.1 操作系统安全方案设计

- Windows 系统安全增强方案
- UNIX/Linux 系统安全增强方案

2.2 网络设备及通信安全方案设计

- 网络设备安全增强方案
- 网络边界安全保护方案
- 网络通信安全保护方案

2.3 计算环境安全方案设计

- 服务器安全增强方案
- 服务器安全监控方案
- 终端安全保护方案

2.4 应用及数据安全方案设计

- 应用安全保护方案
- 数据安全保护方案

2.5 网络安全管理方案设计

- 用户身份认证及访问控制方案
- 网络安全日志数据分析方案
- 网络安全运维管理方案

3. 网络安全设备部署与使用

3.1 防火墙部署与使用

- 防火墙产品技术资料阅读
- 防火墙部署和安装
- 防火墙配置与使用

3.2 IDS/IPS 部署与使用

- IDS/IPS 产品技术资料阅读
- IDS/IPS 部署和安装
- IDS/IPS 配置与使用

3.3 网闸部署与使用

- 网闸产品技术资料阅读
- 网闸部署和安装
- 网闸配置与使用

3.4 VPN 部署与使用

- VPN 产品技术资料阅读
- VPN 部署和安装
- VPN 配置与使用

3.5 漏洞扫描部署与使用

- 漏洞扫描产品技术资料阅读
- 漏洞扫描部署和安装
- 漏洞扫描配置与使用

4. 网络信息系统安全配置与管理

4.1 操作系统安全配置与管理

- Windows 系统安全配置与管理
- Linux 系统安全配置与管理

4.2 数据库系统安全配置与管理

- Oracle 安全配置与管理

- MS SQL 安全配置与管理
- MySQL 安全配置与管理
- 国产数据库安全配置与管理

4.3 网站系统安全配置与管理

- Apache 安全配置与管理
- IIS 安全配置与管理

4.4 网络设备安全配置与管理

- 路由器安全配置与管理
- 交换机安全配置与管理

5. 网站安全需求分析与安全保护工程

5.1 网站安全威胁与需求分析

- 网站安全概念
- 网站安全分析
- 网站安全需求

5.2 Apache 安全分析与增强

- Apache 安装和配置
- Apache 安全分析
- Apache 安全机制理解及配置（文件权限设置、认证和授权、日志配置和读取、IP 地址和域名访问控制）
- Apache 安全漏洞处理办法

5.3 IIS 安全分析与增强

- IIS 安装和配置
- IIS 安全分析
- IIS 安全机制类型及配置（文件权限设置、认证和授权、日志配置和读取、IP 地址和域名访问控制）

- IIS 安全漏洞处理办法

5.4 Web 应用漏洞分析与防护

- SQL 注入漏洞分析与防护
- XSS 漏洞分析与防护
- 目录遍历漏洞分析与防护
- 文件上传漏洞分析与防护

5.5 网站安全保护机制与技术方案

5.5.1 网站构成组件安全加固

- 操作系统安全加固
- 数据库系统安全加固
- Web 应用安全加固
- 网站通信安全加固
- 网站后台管理安全加固
- 网站域名安全加固

5.5.2 网站攻击防护及安全监测

- Web 防火墙
- 网络流量清洗
- Web 入侵检测
- Web 漏洞扫描

6. 云计算安全需求分析与安全保护工程

6.1 云计算安全威胁与需求分析

6.1.1 云计算安全威胁

- 云计算用户安全威胁
- 云计算平台安全威胁
- 虚拟机安全威胁
- 云平台运维安全威胁

6.1.2 云计算安全需求

- 云操作系统安全
- 云服务安全合规
- 多租户安全隔离
- 数据托管
- 隐私保护

6.2 云计算安全保护机制与技术方案

6.2.1 云计算安全等级保护框架

- 云计算保护对象安全等级划分
- 云计算保护对象安全保护方法
- 云计算安全等级保护设计框架

6.2.2 云计算安全防护

- 物理和环境安全（传统的物理环境安全、云计算平台物理位置选择）
- 网络和通信安全［网络通信安全、网络边界安全等，涉及基础设施即服务（IaaS）安全］
- 设备和计算安全［资源控制、镜像和快照保护等，涉及平台即服务（PaaS）安全］
- 应用和数据安全［软件容错、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等，涉及软件即服务（SaaS）安全］
- 云用户安全保护（云用户身份标识与鉴别、云用户访问控制等）

6.2.3 云计算安全管理

- ◆ 安全策略和管理制度
- ◆ 安全管理机构和人员
- ◆ 安全管理对象

6.2.4 云计算安全运维

- ◆ 云计算环境与资产运维管理
- ◆ 云计算系统安全漏洞检查与风险分析
- ◆ 云计算系统安全设备及策略维护
- ◆ 云计算系统安全监管
- ◆ 云计算系统安全监测与应急响应
- ◆ 云计算安全运维安全措施（特权管理、远程访问安全、运维审计、容灾备份等）

6.3 云计算安全保护案例分析

- 云计算安全应用参考案例分析
- 云计算隐私保护技术措施

7. 工控安全需求分析与安全保护工程

7.1 工控系统安全威胁与需求分析

- 工业控制系统概念及组成（SCADA 系统、分布式控制系统、过程控制系统、可编程逻辑控制器、远程终端、数控机床及数控系统等）
- 工业控制系统安全威胁分析（自然灾害及环境、内部安全威胁、设备功能安全故障、恶意代码、网络攻击等）
- 工业控制系统安全隐患类型（工控协议安全、工控系统技术产品安全漏洞、工控系统基础软件安全漏洞、工控系统算法安全漏

洞、工控系统设备固件漏洞、工控系统设备硬件漏洞、工控系统开放接入漏洞、工控系统供应链安全等）

- 工控系统安全需求分析（传统 IT 的安全、控制设备及操作安全、安全管理合规等）

7.2 工控系统安全保护机制与技术

7.2.1 物理及环境安全防护

- 视频监控
- 工业主机加固

7.2.2 安全分区与边界防护

- 安全分区
- 工控防火墙
- 工业控制安全隔离与信息交换系统

7.2.3 身份认证与访问控制

- 多因素认证
- 最小特权
- 避免使用默认口令或弱口令

7.2.4 远程访问安全

- 禁用高风险服务
- 安全加固
- 虚拟专用网络（VPN）
- 安全审计

7.2.5 工控系统安全加固

- 安全配置策略
- 身份认证增强
- 强制访问控制
- 程序白名单控制

7.2.6 工控安全审计

- 安全审计设备部署
- 审计数据备份
- 审计数据分析利用

7.2.7 恶意代码防范

- 防病毒软件测试及部署运行
- 防病毒和恶意软件入侵管理机制
- 重大工控安全漏洞信息获取及其补丁升级措施

7.2.8 工控数据安全

- 工业数据管理方法
- 工业数据安全保护措施（安全隔离、访问控制、加密传输与存储、定期备份等）
- 测试数据保护措施（测试数据保护类型、签订保密协议、回收测试数据等）

7.2.9 工控安全监测与应急响应

- 工控网络安全监测设备安装和使用
- 工控安全事件应急响应预案制定、演练

7.2.10 工控安全管理

- 资产管理
- 冗余配置
- 安全软件选择与管理
- 配置和补丁管理
- 供应链管理

- 落实责任

7.2.11 工控安全典型产品技术

- 工控系统防护类型产品技术原理和部署使用（工控防火墙、工控加密、工控用户身份认证、工控可信计算、系统安全加固等）
- 工控系统物理隔离类型产品技术原理和部署使用（网闸、正反向隔离装置等）
- 工控安全审计与监测类型产品技术原理和部署使用（工控安全审计和工控入侵检测系统）
- 工控安全检查类型产品技术原理和部署使用（工控漏洞扫描、工控漏洞挖掘、工控安全基线检查等）
- 工控运维和风险管控类型产品技术原理和部署使用（工控堡垒机、工控风险管理系统等）

8. 移动应用安全需求分析与安全保护工程

8.1 移动应用安全威胁与需求分析

- 移动操作系统安全分析
- 移动通信网络安全分析
- 移动应用 App 安全分析

8.2 Android 系统安全与保护机制

- Android 系统安全体系
- Android 系统安全机制（进程沙箱隔离机制、SQLite 数据库安全、应用程序签名机制、权

限声明机制、网络传输加密）

8.3 iOS 系统安全与保护机制

- iOS 系统安全体系
- iOS 系统安全机制（安全启动链、权限分离机制、代码签名机制、DEP、地址空间布局随机化、沙箱机制、数据的加密与保护机制、网络传输加密）

8.4 移动应用安全保护机制与技术方案

8.4.1 移动应用 App 安全风险

- 逆向工程风险
- 篡改风险
- 数据窃取风险

8.4.2 移动应用 App 安全加固

- 防逆向、防调试、防篡改
- 数据防泄露、传输数据防护

8.4.3 移动应用 App 安全检测

- 身份认证机制检测
- 通信会话安全机制检测
- 敏感信息保护机制检测
- 日志安全策略检测
- 交易流程安全机制检测
- 服务端鉴权机制检测
- 访问控制机制检测
- 数据防篡改能力检测
- 防 SQL 注入能力检测
- 防钓鱼安全能力检测
- App 安全漏洞检测

8.5 移动应用安全综合应用案例分析

- 金融移动安全
- 运营商移动安全
- 移动办公安全

9. 大数据安全需求分析与安全保护工程

9.1 大数据安全威胁与需求分析

9.1.1 大数据安全威胁分析

- 大数据概念与特点
- 大数据安全问题

9.1.2 大数据安全需求分析

- 数据安全基本要求（数据的真实性、实时性、机密性、完整性、可用性、可追溯性）
- 大数据安全合规
- 大数据跨境安全
- 大数据隐私保护
- 大数据处理平台安全
- 大数据业务安全
- 大数据安全运营

9.2 大数据安全保护机制与技术方案

9.2.1 大数据自身安全保护技术

- 数据源认证
- 数据溯源
- 数据用户标识和鉴别
- 数据资源访问控制

9.2.2 大数据平台安全保护技术

- 大数据平台边界安全

- 大数据网络通信安全
- 大数据用户身份认证与权限管理
- 大数据计算安全
- 大数据平台应急灾备
- 大数据审计与监控

9.2.3 大数据业务安全保护技术

- 业务授权
- 业务逻辑安全
- 敏感数据安全检查

9.2.4 大数据隐私安全保护技术

- 数据身份匿名
- 数据差分隐私
- 数据脱敏
- 数据加密
- 数据访问控制

9.2.5 大数据运营安全保护技术

- 大数据处理系统的安全维护
- 大数据处理系统安全策略更新
- 大数据处理系统安全设备配置
- 大数据处理系统安全事件监测与应急响应
- 大数据处理系统入侵检测与网络安全态势感知
- 大数据处理系统网络攻击取证
- 大数据处理系统安全审计、安全堡垒机
- 大数据处理系统容灾备份

9.2.6 大数据安全管理与标准规范

- 大数据安全等级保护及相关标准规范理解
- 大数据分类分级
- 数据跨境流动安全
- 数据备份与恢复

9.3 大数据安全保护案例分析

- 大数据安全平台及解决方案分析
- 数据安全管理方法理解
- 支付卡行业数据安全规范

三、题 型 举 例

考试科目 1：网络信息安全基础知识和技术

1. 攻击者利用 John the Ripper 工具对目标服务器进行攻击，则此攻击者所利用的方法是__（1）__。

（1）A．会话劫持　　B．口令破解

C．端口扫描　　D．拒绝服务

2．VPN 产品的安全实现技术主要是__（2）__。

（2）A．RFC、IPSec　　B．XML、BGP

C．SSL、IPSec　　D．BGP、OSPF

3．网络中的明文传输容易造成信息泄露，为了抵御网络监听，常用的技术方法是__（3）__。

（3）A．SSL、OSPF　　B．IPSec、SNMP

C．SSL、IPSec　　D．OSPF、SNMP

4．Network firewalls operate at different layers of the __(4)__ and TCP/IP network models. The lowest layer at which a firewall can operate is the third level which is the network layer for the OSI model and the Internet Protocol layer for TCP/IP. At this layer a firewall can determine if a packet is from a __(5)__ source but cannot grant or deny access based on what it contains. Firewalls that operate at the highest layer， which is the application layer， know a large amount of information including the source and the packet __(6)__. Therefore， they can be much more selective in granting access. This may give the impression that firewalls functioning at a higher layer must be better， which is not necessarily the case. The lower the layer at which the packet is intercepted， the more secure the system is. If the __(7)__ cannot get past the third layer， it is impossible to gain control of the operating system.

Application level gateways or proxies operate at the application layer. Packets received or leaving cannot access services for which there is __(8)__. Stateful multilayer inspection firewalls combine aspects of the other three types of firewalls.

(4) A. OSI　　B. ISO
　　C. SMTP　　D. IDS
(5) A. active　　B. old
　　C. trusted　　D. new
(6) A. virus　　B. address
　　C. contents　　D. password
(7) A. dog　　B. bird
　　C. intruder　　D. tiger

（8）A．no proxy　　B．no OS
C．no VPN　　D．no Desktop

考试科目 2：网络信息安全工程与综合应用实践

试题一（10 分）

某公司网站应用架构采用 LAMP 模式，其操作系统为 Linux，Web 服务器采用 Apache HTTP，数据库是 MySQL，应用编程则为 PHP，试解决网站应用中的安全问题。

（1）已知管理员使用 Telnet 和 HTTP 远程管理网站服务器，而国家信息安全等级安全保护要求为：（5 分）

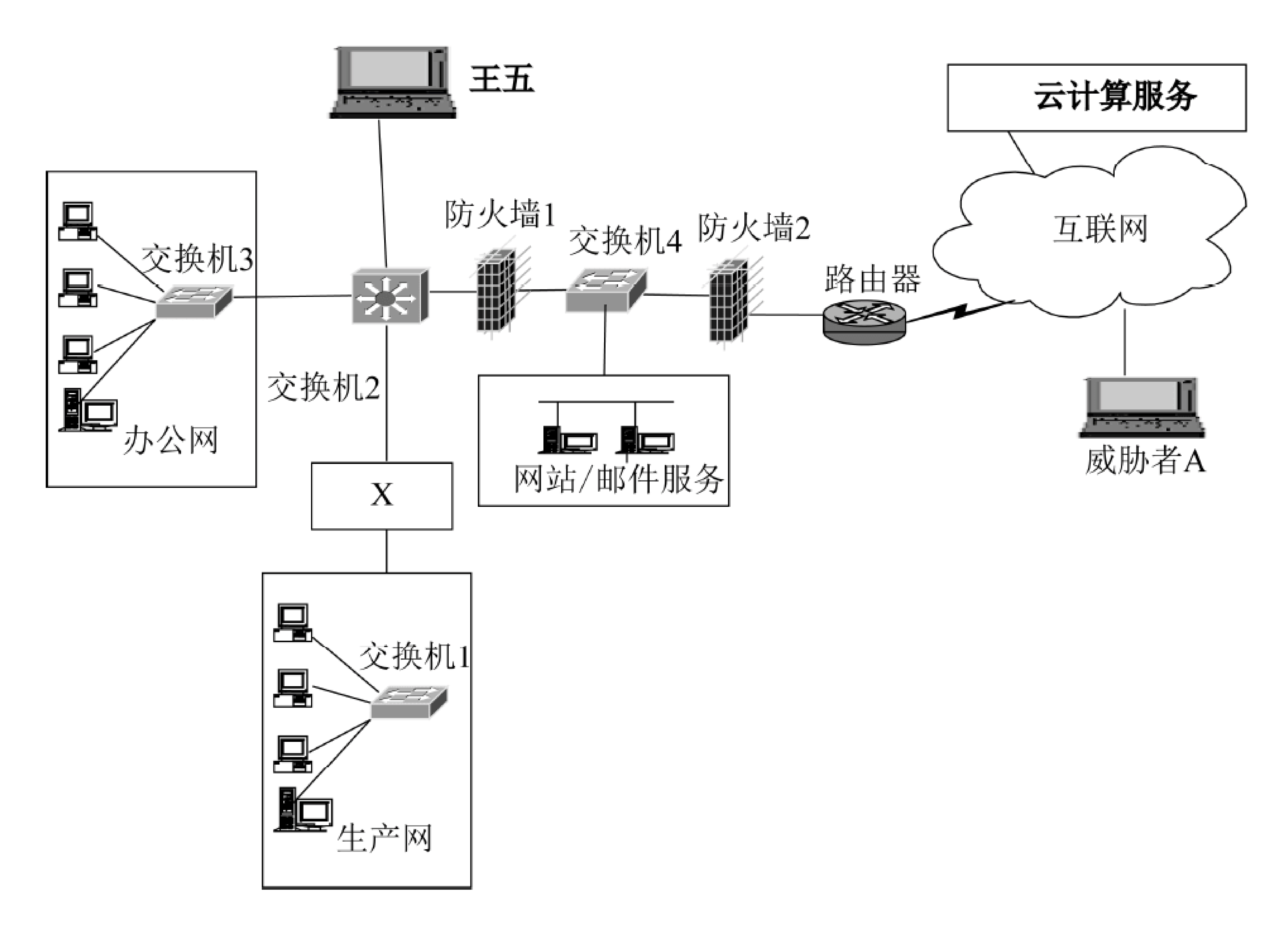
- 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。
- 应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。

请问：采取什么安全措施可以符合等级保护要求？如何获取网站操作系统和数据库的用户信息？

（2）网站安全策略要求网站的默认服务端口改成 8081，远程计算机的 IP 地址为 192.168.0.2，若要其可以访问网站服务器/www/admin 资源。如何配置 Apache 相关文件以符合安全策略要求？（5 分）

试题二（25 分）

已知甲公司网络环境结构如下图所示，请根据图中信息及问题要求，回答问题（1）至问题（4），将解答填入答题纸的对应栏内。



（1）公司为了防止生产网受到外部的网络安全威胁，安全策略要求生产网和外部网之间部署安全隔离装置，隔离强度达到接近物理隔离。请问：X 最有可能代表的安全设备是什么？简要描述该设备的工作原理。（6 分）

（2）公司拟购买云计算服务，并租用虚拟主机，请列举云计算的服务安全风险类型。（5 分）

（3）公司的防火墙是否能有效地保护虚拟主机安全？为什么？（4 分）

（4）高级持续威胁（简称 APT）常常利用电子邮件，开展有针对性的目标攻击，威胁者 A 发送带有恶意 Word 附件的电子邮件到公司邮件服务器，等待邮件接收者执行电子邮件附件，触发恶意程序运行，从而渗透到甲公司内部网络，请给出威胁者 A 的攻击流量经过的网络设备。针对 APT，可以部署什么安全设备来自动检测？该设备的主要技术方法是什么？（10 分）